IN THE DRAWINGS

A Transmittal of Replacement Sheets of Formal Drawing accompanies this Reply to add a "Prior Art" legend to Figs. 1-4.

REMARKS

The Applicants request reconsideration of the rejection.

Claims 1-17 are pending.

The Examiner objected to Figures 1-4, requiring them to be designated by a legend --Prior Art--. A Transmittal of Replacement Sheets of Formal Drawing accompanies this Reply, under cover of which the amended figures are submitted.

The Examiner also objected to the drawings as including reference characters not mentioned in the description, as set forth on Pages 2-3 of the Office Action. The specification has been amended to include the reference characters shown in the drawings.

The Examiner also objected to the disclosure as containing the minor informalities on set forth on Pages 3-4 of the Office Action. The specification has been amended to address the Examiner's concerns.

Claims 1-8 were rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over Claim 14 of U.S. Patent No. 6,615,354 in view of Jaffe et al., U.S. 6,510,518. Without admitting to the propriety of the rejection, which appears to be based on an incorrect interpretation of Jaffe (see the discussion below), a Terminal Disclaimer is being submitted with this paper to expedite the examination and allowance of the claims.

Claims 1-8 were rejected under 35 U.S.C. 112, second paragraph, as being indefinite for the reasons set forth on Pages 6-7 of the Office Action. The Applicants have amended the claims to address the Examiner's concerns.

Claims 1-8 were also rejected under 35 U.S.C. 103(a) as being unpatentable over the Applicant's Admitted Prior Art (AAPA) in view of Jaffe et al., 6,510,518 (Jaffe). The Applicants traverse as follows.

Jaffe discloses a cryptographic method that uses a constant Hamming weight representation of data in its internal operations, such that the Hamming weight of all input values is constant. Thus, according to Jaffe, the data to be manipulated at the bit level differs from the traditional binary representation of the numbers being manipulated. Specifically, in hardware, bit values of 1 and 0 can be represented, for example, by a voltage level on a wire, by a charge in a capacitor, or by the state of a transistor switch.

Jaffe's method is very useful for protecting the data against Side-Channel Attacks, for example, a SPA attack (Simple Power Analysis) or a DPA attack (Differential Power Analysis), which makes it possible to infer the value of the data by observation of current consumption, because the data to be processed itself is plural bits of information using a constant Hamming weight.

In accordance with a prior technology shown in the present specification, in order to improve tamper resistance, data to be processed is first transformed by using data for disturbance, so the degree of correlation between the magnitude of a current consumed during the processing and the original data is lowered. The transformed data is then processed. Finally, a result of the processing is subjected to inverse transformation by using the data for disturbance or by using a result of processing the data for disturbance to produce a value equal to data which will be obtained as a result of processing the original data. See page 21, lines 1-12 of the specification.

Thus, while Jaffe is very useful for protecting the data against Side-Channel Attacks because the data itself to be processed is expressed in the form of plural bits of information using a constant Hamming weight in hardware, if Jaffe is combined with AAPA, the Hamming weight for the data itself to be processed may directly be made constant. However, there is no suggestion to make constant the Hamming weight for the data for disturbance, which indirectly improves the tamper resistance for the data itself to be processed. That is, merely combining AAPA with Jaffe does not lead the person of ordinary skill to make constant the Hamming weight for the data for disturbance.

In view of the foregoing amendments and remarks, the Applicants respectfully request reconsideration of the rejection and allowance of the claims.

Respectfully submitted,

Daniel J. Stanger
Registration No. 32,846
Attorney for Applicants

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 Diagonal Road, Suite 370
Alexandria, Virginia 22301
(703) 684-1120
Date: April 3, 2006